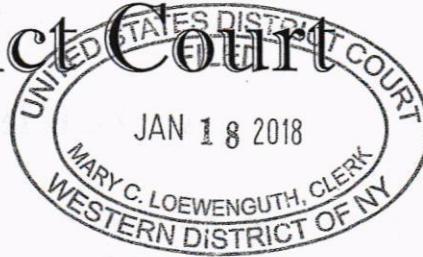


United States District Court

for the
Western District of New York



United States of America

v.

Case No. 18-MJ- 511

DAVID D. BLASZAK

Defendants

CRIMINAL COMPLAINT

I, NICHOLAS MELCHIORRE, Special Agent with the United States Department of Homeland Security, Criminal Investigations Unit, the complainant in this case, state that the following is true to the best of my knowledge and belief:

On or about and in between September 1, 2015 through the PRESENT, in the Western District of New York, the defendant **DAVID D. BLASZAK** violated 18 U.S.C. §§ 2252A(a)(2)(A) & 2252A(a)(5)(B), offenses described as follows:

the defendant knowingly received child pornography that has been mailed or, using any means or facility of interstate or foreign commerce, been shipped or transported in or affecting interstate or foreign commerce by any means, including by computer in violation of Title 18, United States Code, Section 2252A(a)(2)(A); and possession of child pornography, in violation of Title 18, United States Code, Section 2252A(a)(5)(B).

SEE ATTACHED AFFIDAVIT OF NICHOLAS MELCHIORRE, S.A., H.S.I.

This Criminal Complaint is based on these facts:

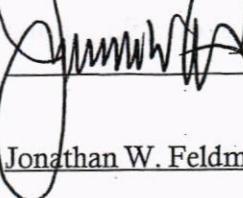
- Continued on the attached sheet.

Sworn to before me and signed in my presence.

Date: January 18, 2018

City and State: Rochester, New York


NICHOLAS MELCHIORRE, S.A. U.S. H.S.I.
Complainant's signature
Printed name and title


Jonathan W. Feldman, United States Magistrate Judge
Printed name and title
Judge's signature

AFFIDAVIT IN SUPPORT OF A CRIMINAL COMPLAINT

STATE OF NEW YORK)
COUNTY OF MONROE) SS:
CITY OF ROCHESTER)

NICHOLAS MELCHIORRE, being duly sworn, deposes and says:

1. I am a Special Agent ("SA") with the Department of Homeland Security ("DHS"), United States Immigration and Customs Enforcement ("ICE"), Homeland Security Investigations ("HSI"), and am presently assigned to the HSI Buffalo, NY office. I have been employed as a federal law enforcement officer since November 2010. As a Special Agent, I am a federal law enforcement officer within the meaning of Rule 41(a) of the Federal Rules of Criminal Procedure, that is, an officer of the United States who is empowered by law to conduct investigations of, and to make arrests for, federal criminal offenses.

2. I have participated in investigations involving the production, receipt, distribution and possession of child pornography, in violation of Title 18, United States Code, Section 2251(a), Section 2252A(a)(2)(A) and Title 18, United States Code, Section 2252A(a)(5)(B). I have received specialized training in the area of child pornography and child exploitation investigations, and I have had the opportunity to observe and review numerous images and videos of child pornography, as defined in Title 18, United States Code, Section 2256.

3. This affidavit is submitted for the limited purpose of establishing probable cause to believe that DAVID D. BLASCZAK, did knowingly receive and distribute child

pornography that had been transported in and affecting interstate or foreign commerce by computer, in violation of Title 18, United States Code, Section 2252A(a)(2)(A), and did knowingly possess and access with intent to view child pornography that had been transported in and affecting interstate or foreign commerce by computer, in violation of Title 18, United States Code, Section 2252A(a)(5)(B).

4. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. Because this affidavit is submitted for the limited purpose of establishing probable cause to support a criminal complaint, it does not include each and every fact known to me concerning this investigation.

5. In March 2012, HSI Phoenix initiated an investigation into a password-protected, fee-based "Website M"¹ after a consensual interview with a suspect in a child exploitation investigation ("S1"). The interview resulted in HSI agents assuming S1's online identity on Website M, which is a closed site that can only be accessed by members who were provided login information by Website M.² HSI Phoenix SAs determined that Website M advertises files of child exploitative material for purchase.

¹ The actual name of Website M is known to law enforcement. However, the investigation into the users of Website M remains ongoing, and the disclosure of the name of Website M would potentially alert their members to the fact that law enforcement officers are investigating Website M. Public disclosure of that fact is likely to provoke members to notify other members of the investigation, flee, and/or destroy evidence. Accordingly, to preserve the confidentiality and integrity of the ongoing investigation, the actual names and other identifying details of Website M are not disclosed in this affidavit.

² S1 provided SAs with the URL link to Website M and S1's login information to Website M but S1 has not provided sufficient information to law enforcement to understand how S1 originally obtained the URL or login information for Website M.

6. Results from the preliminary investigation indicated that Website M was being hosted on a server physically located in India, and the website claimed to offer 600,000 images and 400 hours of video, all of which could be downloaded for a fee as compressed, encrypted files (.RAR files). Website M typically charged \$89.99 USD for each .RAR file. Once downloaded, the user could “un-compress” the .RAR file to reveal multiple image and/or video files. It appeared to HSI Phoenix SA Nicole Rye that most of the .RAR files contain between 500 and 2,000 image and/or video files. Law enforcement agents who visited Website M estimated that many of the images and videos advertised on the website depict pre-pubescent male and female minors engaged in sexual activity with adults and/or posed in a sexually explicit manner.

7. According to SA Rye, Website M allows members to preview samples of the images/videos contained in the .RAR file prior to purchasing the .RAR file. Over the course of their investigation, which has involved previewing and downloading multiple .RAR files, law enforcement has found that the “sample” images/video screenshots SAs previewed always corresponded to the un-compressed image and video files contained in the downloaded .RAR file.

8. After selecting an encrypted .RAR file, the member pays for its password by entering in credit card information. Website M then causes an email to be sent to the member with the encryption password for the .RAR file. The member must enter that password to decrypt and un-compress the .RAR file.

9. I have been informed by SA Rye that, as a result of the interview with S1, law enforcement obtained membership information to Website M that allowed law enforcement

to pose as S1 on the website. Between April 2014 and May 2017, SAs made multiple undercover purchases of .RAR files from Website M.

10. For example, in April 2014, SAs (posing as S1) successfully downloaded .RAR files from Website M. SAs reviewed the un-compressed image files and, based upon an analysis of hash values, law enforcement determined that the purchased files included video and image files from what law enforcement refer to as the “Jenny” series. The United States-based National Center for Missing and Exploited Children has identified and verified that the images from the “Jenny” series images depict a pre-pubescent minor child who appears to be less than ten years of age. Purchased files included the following video and image files of “Jenny”:

- a) “180-2.AVI 9Yo Jenny licked by dog. 16min./with sound.” The screenshot for this video depicts a nude, blindfolded, pre-pubescent female who appears to be less than ten years of age lying on her back while a dog licks her genitals; and
- b) Over twenty pictures from the “Jenny” series including an image of the same pre-pubescent, nude, female performing fellatio on a dog.

11. On May 26, 2017, an HSI Phoenix SA, working in an undercover capacity purchased a .RAR file from Website M titled “SIBERIAN MOUSE #36.” The un-compressed files contained in the .RAR file depicted what appeared to be minors engaged in sexually explicit acts. When the SA purchased the SIBERIAN MOUSE #36” file, the SA received a confirmation email from an email address from a U.S. payment processor, hereinafter PAYMENT PROCESSOR, stating that “Your order is currently being processed.” The identity of the PAYMENT PROCESSOR is known, but is being left out of

this affidavit due to the ongoing investigation of Website M and the PAYMENT PROCESSOR.

12. According to SA Rye, HSI Phoenix SAs initiated an investigation into the link between the PAYMENT PROCESSOR and Website M. The PAYMENT PROCESSOR was identified as a payment processor and online business management tool used by Website M.

13. On July 31, 2017, a Federal Magistrate for the District of Arizona signed a search warrant for the electronic documents in the possession of the PAYMENT PROCESSOR related to their business transactions with and on behalf of Website M.

14. On August 11, 2017, the PAYMENT PROCESSOR provided several spreadsheets in compliance with the search warrant. One of the spreadsheets listed all the transactions that had been processed by the PAYMENT PROCESSOR on behalf of Website M. This list included over 1,000 purchases made to Website M.

15. In September 2017, SA Rye analyzed the PAYMENT PROCESSOR records and identified individuals who made multiple purchases from Website M. The PAYMENT PROCESSOR records indicate that David Blasczak ("BLASZAK") made approximately ten purchases from Website M between September 2015 and April 2017. According to the PAYMENT PROCESSOR records, the email address to which it sent the auto-generated receipts and passwords for purchases made by BLASZAK on Website M was blasczakd@gmail.com.

16. In response to a summons, PayPal Holdings, Inc. provided the following subscriber information associated with the David Blasczak purchaser:

First Name: David

Last Name: Blasczak

Email: blasczakd@gmail.com

Address: [REDACTED]

4 West Genesee Street, Clyde, NY, 14433

2 West Genesee Street, Clyde, NY, 14433

Frequent IP Addresses: 98.10.10.158 (SUSPECT IP ADDRESS).

17. In response to a summons, Charter Communications provided information that between February 17, 2017 through April 11, 2017, the SUSPECT IP ADDRESS was subscribed to BLASCZAK at [REDACTED]

18. Based upon the PAYMENT PROCESSOR records, law enforcement generated the following list of BLASCZAK's purchases made via the PAYMENT PROCESSOR from Website M along with identifying information linked to each purchase:

Date	Title	First Name	Last Name	Email	Phone	Region	Postal
9/23/2015	PHP SCRIPT 153	David	Blasczak	<u>blasczakd@gmail.com</u>	3154813450	NY	14513
2/17/2017	PHP SCRIPT 347	David	Blasczak	<u>blasczakd@gmail.com</u>	3154813450	NY	14513
2/19/2017	PHP SCRIPT 133	David	Blasczak	<u>blasczakd@gmail.com</u>	3154813450	NY	14513
2/19/2017	PHP SCRIPT 218	David	Blasczak	<u>blasczakd@gmail.com</u>	3154813450	NY	14513
2/21/2017	PERL SCRIPT 113	David	Blasczak	<u>blasczakd@gmail.com</u>	3154813450	NY	14513
2/22/2017	AJAX SCRIPT 79	David	Blasczak	<u>blasczakd@gmail.com</u>	3154813450	NY	14513
3/3/2017	AJAX SCRIPT 83	David	Blasczak	<u>blasczakd@gmail.com</u>	3154813450	NY	14513
4/8/2017	PHP SCRIPT 269	David	Blasczak	<u>blasczakd@gmail.com</u>	3154813450	NY	14513
4/10/2017	AJAX SCRIPT 27	David	Blasczak	<u>blasczakd@gmail.com</u>	3154813450	NY	14514
4/11/2017	PHP SCRIPT 412	David	Blasczak	<u>blasczakd@gmail.com</u>	3154813450	NY	14513

19. After obtaining BLASCZAK's purchase history from the PAYMENT PROCESSOR, an HSI Phoenix SA, in an undercover capacity, viewed "samples" from each file titled in BLASCZAK's purchase records from Website M. The previews were recorded

using screen capture software available to law enforcement. I have reviewed previews from some of the files referenced in the table above, which BLASZCZAK downloaded. Based on my review they contain child pornography as defined by Title 18, United States Code, Section 2256(8).

20. Specifically, on April 11, 2017, BLASZCZAK purchased a .RAR file with the billing code "PHP SCRIPT 412." SAs located a .RAR file on Website M titled "HM VIDEO ARCHIVE 412." When SAs clicked on this .RAR file on Website M, the website provided the following prompt at the bottom of the webpage "BUY NOW PASSWORD FOR HM VIDEO ARCHIVE" #412." When SAs clicked on this prompt, the webpage displayed an option to buy "PHP SCRIPT 412" with an "Immediate License Code sent by Email. I reviewed the screen capture of the "samples" viewed from PHP SCRIPT 412 file. Two of the image files are described below:³

- a) The first image depicts a pre-pubescent, Caucasian minor female who appears to be less than ten years of age sitting on a couch and wearing what appears to be a bathrobe. The child's right hand is touching her genitals and the focus of the picture is on her genitals and chest.
- b) The second image depicts a pre-pubescent female Caucasian child who appears to be less than 8 years of age. There is an adult male penis inserted into her mouth.

21. In addition, on April 10, 2017 BLASZCZAK purchased a .RAR file with the billing code "AJAX SCRIPT 27." SAs located a .RAR file on Website M titled "NU PHOTO ARCHIVE 27, Pre-Teen Hardcore #8. 2020 images." When SAs clicked on this .RAR file

³ The image files are not associated with individual file names because they were previewed as "samples." If law enforcement had downloaded the .RAR file, the un-compressed files would contain individual file names. Law enforcement elected not to download all of the .RAR files purchased by BLASZCZAK because law enforcement was concerned that such a large volume of purchases would be suspicious to Website M and may cause Website M to terminate S1's membership.

on Website M the webpage displayed an option to buy "AJAX SCRIPT 27" with an "Immediate License Code sent by Email." I reviewed the screen capture of the "samples" viewed from AJAX SCRIPT 27 file. Two of the image files below:

- a) The first image depicts a pre-pubescent, Caucasian minor⁴ who appears to be less than ten years of age sitting thigh to thigh with an adult male. The genital area of the child is touching the adult male. The minor child is holding the adult male's penis in the child's hand.
- b) The second image depicts a Caucasian female who appears to be less than ten years of age sitting on her knees on top of a blanket. The lower body of an adult male is visible and he appears to be standing over the female child. The adult male's penis is inserted into the child's mouth.

22. Based on my training and experience, and my investigation of this case, it appears that Website M generates a billing name for files containing child pornography to disguise the contents of the file for anyone with access to the billing records, such as the payment processor. As indicated in the chart above, all purchases appear to be "script." The names of the "script" are the same as legitimate "script" that computer programmers utilize such as JAVA. Website M registered their business with the PAYMENT PROCESSOR as "The Scripts."

23. I reviewed the financial purchase records provided by the PAYMENT PROCESSOR and noted that BLASCZAK's purchases listed his billing address as [REDACTED]
[REDACTED] [REDACTED]

⁴ Due to the close up nature of the photo it is not possible to tell if the minor is male or female.

24. Based on the above, a search warrant was signed on January 16, 2018 by Hon. Jonathan Feldman, United States Magistrate Judge, authorizing a search of [REDACTED], the home of BLASZAK.

25. On January 18, 2018, Agents from HSI, accompanied by members of the New York State Police, executed the above-described search warrant at [REDACTED], the home of BLASZAK. Upon executing the warrant, Agents located several digital devices including a laptop, a digital camera, multiple SD cards, multiple thumb drives, and 2 sandisk memory sticks. One of the devices is an "Infinitive" 64 gigabyte USB thumb drive, serial number BN160625517B, found in a brief case near the front entranceway of the residence. An HSI Computer Forensic Agent (CFA), previewed the contents of the thumb drive on scene and immediately discovered images and videos of child pornography involving prepubescent minors. At the time of this writing, the CFA already discovered approximately 10 gigabytes of files on the subject thumb drive containing suspected child pornography. I have described two of the images and one video below:

- a. Image file located in "folder 01," jpg. file "2," created 9/6/17, which depicts a prepubescent female with her legs spread, inserting her fingers into her vagina;
- b. Image file located in "folder 01," jpg. file "2011-05-24_12-42-53_Zdjcie0061," created 9/6/17, which depicts a prepubescent female, approximately 2 years of age performing oral sex on an adult male. The male's penis is seen in the child's mouth;
- c. Video file located in "folder 362 vid," .avi file "362-7," created 2/12/17, which depicts an adult male performing oral sex on a prepubescent female. The female appears to be approximately 3 years of age and the males mouth can be seen in contact with the child's vagina.

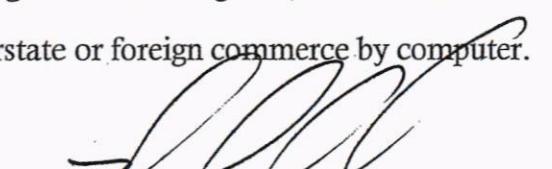
26. Agents estimate that they have already discovered in excess of 1,000 images and multiple videos of child pornography on the subject thumb drive. The thumb drive and other digital devices are currently being transported to HSI Buffalo for a full forensic review.

27. BLASCZAK was present during the execution of the search warrant and was interviewed by HSI SAs Justin Burnham and Nicole Rye. The interview took place in SA Burnham's vehicle outside of the residence. During that interview, BLASCZAK initially denied having any images or videos of child pornography. He then admitted to being the sole owner and user of the email account and credit card associated with receipt of child pornography through Website M (blasczakd@gmail.com). As the conversation progressed, BLASCZAK acknowledged that he owned a thumb drive that contained images and videos of child pornography. He then directed Agents to the brief case and thumb drive described above. BLASCZAK admitted that he purchased child pornography over the internet, and that the website that he purchased child pornography from required that he create an account containing a username and password. BLASCZAK admitted that he would pay approximately \$100 per file that he purchased. It should be noted that since Website M sold compressed files, it is estimated that each "file" BLASCZAK purchased for \$100 would have contained thousands of images and/or videos. BLASCZAK estimated that the children depicted in the child pornography that he purchased were between 5 and 10 years of age. BLASCZAK specifically used the word "prepubescent," when asked the ages of the children depicted in the videos and images he possessed. BLASCZAK told Agents that he possessed more than 50 videos and hundreds of images on the aforementioned thumb drive. When asked what his favorite type of child pornography was, BLASCZAK stated "oral."

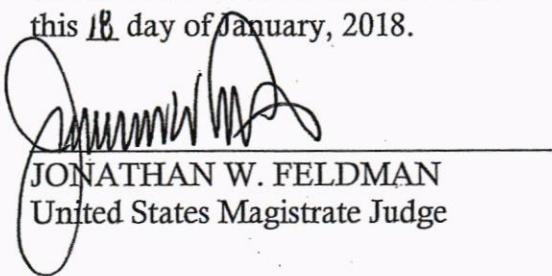
28. As the conversation continued, BLASZCZAK acknowledged that he works as a physician and treats children at his office located at 4 West Genesee Street, Clyde, NY, 14433. BLASZCZAK denied ever abusing any of his child patients, but admitted to Agents that he previously photographed the genitals of children at his office. When asked, BLASZCZAK claimed that he was conducting his own independent research about child sex abuse and paid the parents of approximately 8 children to photograph the children's genitals. BLASZCZAK told Agents that he told the parents that he was conducting medical research. BLASZCZAK admitted that he was not sanctioned by a hospital, university, medical organization or any other professional medical board to photograph children's genitals. He claimed that he took the images for "teaching purposes" but admitted that he kept the photographs for himself for his "own gratification." BLASZCZAK said that the photographs were taken years ago, but that he maintained some photographs of children's genitals in a "teaching" file in his office at his office at 4 West Genesee Street, Clyde, NY, 14433. BLASZCZAK provided a written consent to the seizure of these items. Based on his consent, the items have been seized and will be searched pending the issuance of a search warrant.

29. BLASZCZAK thereafter accompanied agents to NYSP Lyons, where he continued to be interviewed. There, BLASZCZAK made further admissions, including to engaging in sexually abusive behavior against his (deceased) daughter's minor friends during sleepovers. BLASZCZAK stated that he touched his daughter's minor friends while they were sleeping and photographed them. BLASZCZAK admitted to being sexually aroused by his daughter's friends. BLASZCZAK also admitted that he has masturbated to the photographs that he took of his child-patients at his medical practice.

30. Based on the foregoing, I respectfully submit that there is probable cause to believe that DAVID D. BLASZAK has violated Title 18, United States Code, Section 2252A(a)(2)(A), knowingly receiving child pornography that had been transported in and affecting interstate or foreign commerce by computer; and Title 18, United States Code, Section 2252A(a)(5)(B), knowingly possessing and accessing with intent to view child pornography that had been transported in interstate or foreign commerce by computer.


NICHOLAS MELCHIORRE
Special Agent
Homeland Security Investigations

Subscribed to and sworn before me
this 18 day of January, 2018.


JONATHAN W. FELDMAN
United States Magistrate Judge